

**Paper Reference 20158K**  
**Pearson BTEC**  
**Level 3 Nationals Diploma,**  
**Extended Diploma**

**INFORMATION TECHNOLOGY**  
**UNIT 11: CYBER SECURITY AND**  
**INCIDENT MANAGEMENT**

**(PART B)**

**Window for supervised period:**

**Monday 29 April 2019 – Friday 17 May 2019**

**Supervised hours: 4 hours (plus your additional  
time allowance)**

**SET TASK BRIEF**

## **SET TASK BRIEF**

### **PROJET SERENDIPITY**

**Projet Serendipity (PS) is an independent, non – profit organisation formed in 2018, which tries to make links between PhD students. Its joint Chief Executives are Professor Fred Gorse, an expert in artificial intelligence, and Professeur Adele Lefebvre, who studies complex data processing.**

**PS was formed for PhD students to work on computing projects. It now involves over 20 universities around the world and has several PhD students working with it.**

**PS occupies four rooms on the second floor of a building owned by the Pan – Europe Foundation for Education Research (PEFER), based in Lille, France. PS has meeting rooms and workspace but most PhD students work from home, accessing the servers and data stores remotely.**

**The PS board is elected from present PhD students and their supervisors. Fred and Adele provide oversight and continuity, other board members deal with the day – to – day running of PS and its research programme.**

**Turn over**

## **CLIENT BRIEF**

**You advised Fred and Adele on cyber security matters. Now, six months later, Adele has asked you to review the investigation of a cyber security incident.**

**Three months ago Adele saw an article on the MondeLePlusÉtrange.fr ('Strangest World' in English) website. The article was about a coincidental link between different areas of science and had obviously been written about some of PS's work.**

**A week later another article appeared, and then another the following week. Each one based on PS's work.**

**Adele discussed the matter with Fred and they decided to investigate. In particular to find if MondeLePlusÉtrange was accessing that information from the PS network.**

**The investigation team was:**

- **Professeur Adele Lefebvre**
- **Mlle Marina Maubour, a PhD student living in Lille**
- **M. Anton Bernoul, the senior IT Manager at PEFER.**

The investigation took 10 days, during which time two more articles appeared on MondeLePlusÉtrange.

The articles then stopped and no more have been published.

The investigation was inconclusive, although several security matters were addressed during it.

Adele believes that whoever was involved was scared off by the investigation.

---

continued on the next page . . .

**EVIDENCE ITEMS FROM THE SECURITY INCIDENT  
AT PS**

**Evidence items include:**

- 1) Adele's account**
  - 2) Marina's report**
  - 3) Report from PEFER's senior IT Manager**
  - 4) WiFi map and notes**
  - 5) Cyber security document – incident management policy.**
- 

**continued on the next page . . .**

## **1 ADELE'S ACCOUNT**

**PS had only been in its new location for a few weeks when a friend emailed me the URL of an article in MondeLePlusÉtrange. The article was about an unexpected link between two different areas of science. My friend knew about PS and thought I'd be interested.**

**I wasn't expecting much. MondeLePlusÉtrange is mainly 'click – bait'. Its articles are mostly true but twist ordinary events into something that sounds sensational. The headline on the article was 'Astounding Coincidence!!! You'll never guess how these two things are linked'.**

**Anyway, I had a look and really was astounded, the material was something we'd discovered at PS only the previous month. There were no names and the whole thing was vague as to when or where it had happened, but I recognised it straight away.**

**I raised the matter at our next board meeting, two days later. We decided that there was not much we could do. Perhaps one of our research students had talked about their work, or someone had overheard something.**

It could even have been an independent discovery, although it seemed unlikely that it would be announced through MondeLePlusÉtrange.

I emailed MondeLePlusÉtrange, explaining PS, and asked to meet the author to discuss the article.

MondeLePlusÉtrange replied saying they never reveal sources, the author was a staff journalist, and they did not wish to discuss the matter.

Then three more articles were published, one a week. We were certain by then that someone was getting information from PS, so we started an investigation. It was still possible that a student had talked, but we didn't think that anyone could have been involved with everything in all three articles.

I was nominally in charge of the investigation but the work was mainly done by Anton and Marina. The articles finally stopped after number five. By that time the investigation was being talked about by everyone in PS and I think we scared off whoever was involved.

---

continued on the next page . . .

## **2 MARINA'S REPORT**

**Adele asked me to represent PS in the investigation. I live in Lille and often work in the building and I get on well with Anton. I have a good idea of how the PS system works, but I'm no expert with cyber security, so Anton and his team did the technical bits.**

**Anton asked me to help by:**

- a. Taking a WiFi signal reader and my smartphone to find where I could locate the PS WiFi and log in, both inside and outside the building. There was a good signal inside as expected but it was difficult to get a reliable connection outside. I've drawn a map (SEE EVIDENCE ITEM 4) that Anton has used in his report.**
- b. Checking the computer files to see when relevant files were last accessed. That was inconclusive. I knew which research had been referenced by the articles and I'm sure that none of the more obvious files had been looked at recently. Things like progress reports and grant applications.**

**continued on the next page . . .**

**Turn over**

The problem is that data files get used all the time, so it was impossible to say if there had been unauthorised access. All the data is encrypted, so I don't think anyone could have used them even if they did get into the data stores.

- c. Checking the paper files. To see what files had been updated recently. They might have been left on a desk or in the printer for a visitor to see. There were several relevant files, all of them progress reports. Most would have been used at the previous board meeting, or sent in support of grant applications. Someone would have been in the building when they were printed but it's possible that the documents could have been unattended for a while. They're not really that secret. Anton checked the print dates against the PEFER visitor log but didn't find anything.
- 

continued on the next page . . .

### **3 REPORT FROM PEFER'S SENIOR IT MANAGER, M. ANTON BERNOUL**

#### **INVESTIGATION INTO A POSSIBLE DATA BREACH AT PROJET SERENDIPITY (PS)**

**At the request of Professeur Adele Lefebvre, I looked into ways in which information might have been obtained from PS. I investigated six routes.**

- a) PEFER and PS personnel**
- b) Visitors**
- c) Malware**
- d) The PS WiFi system**
- e) Software faults and misconfiguration**
- f) Hardware faults and misconfiguration**

#### **a) PEFER AND PS PERSONNEL**

**PEFER. All of our staff, academic and service, have been with PEFER for at least three years. There have been no similar incidents with PEFER data. I think it impossible that any member of the academic staff is involved. I think it extremely unlikely that any of the service staff are involved. A possible route might be if someone put documents in the general waste rather than shredding it.**

**Turn over**

**PS. Professeur Lefebvre has stated that she does not think that all of the students handling the materials referred to in the articles could have been overheard, or have left papers laying around. The PEFER security log shows that most students had not been in the building in the month before the first article.**

### **b) VISITORS**

**The PEFER security log for the month before the first article shows all the visitors had made an appointment. All visitors were escorted to the correct room by a member of the security staff.**

### **c) MALWARE**

**My team scanned the PS system, including the backup store and any mobile devices and portable storage devices that were available. Nothing was found.**

**continued on the next page . . .**

**d) THE PS WIFI SYSTEM  
NETGEAR ProSAFE WAC730  
using 802.11ac**

I asked Mlle Maubour to survey WiFi signals in the building and surrounding area. She reported that she could get a signal for some distance but no reliable connection at more than a few metres from the building. Her map is included (SEE EVIDENCE ITEM 4).

The outside of the PEFER building is covered by CCTV, so I think it unlikely that an attacker would risk being seen on the street and the area is a no parking zone. It is possible that someone was in a nearby building, such as one of the cafes, but Mlle Maubour could not log in from that distance.

**e) SOFTWARE FAULTS AND MISCONFIGURATION**

All system software had the latest patches and I could not find any configuration errors.

continued on the next page . . .

**f) HARDWARE FAULTS AND MISCONFIGURATION**

**No physical faults were found but two other issues were identified.**

- (i) The WiFi access point had not been patched since 2017, it seems to have been missed out when the system was set up. I don't think there have been any WPA2 vulnerabilities found since then, but I cannot be certain. I reset the WAP to factory settings and then patched everything up to the latest versions. I also made the password more secure. I thought Projet2019 was a bit flimsy.**
- (ii) The router, Cisco 7200. I left a network monitoring tool running for a couple of days to see if there was any suspicious traffic. I was surprised to find that the router itself was sending a signal at 0200 each morning. I checked again over several days to make sure. The signal went to 29.101.211.195 and seemed to be an attempt to report in.**

**continued on the next page . . .**

**Turn over**

There was no reply. I pinged the address and got this:

```
PING 29.101.211.195 (29.101.211.195)  
56(84) bytes of data.  
--- 29.101.211.195 ping statistics ---  
3 packets transmitted, 0 received,  
100% packet loss, time 1999ms
```

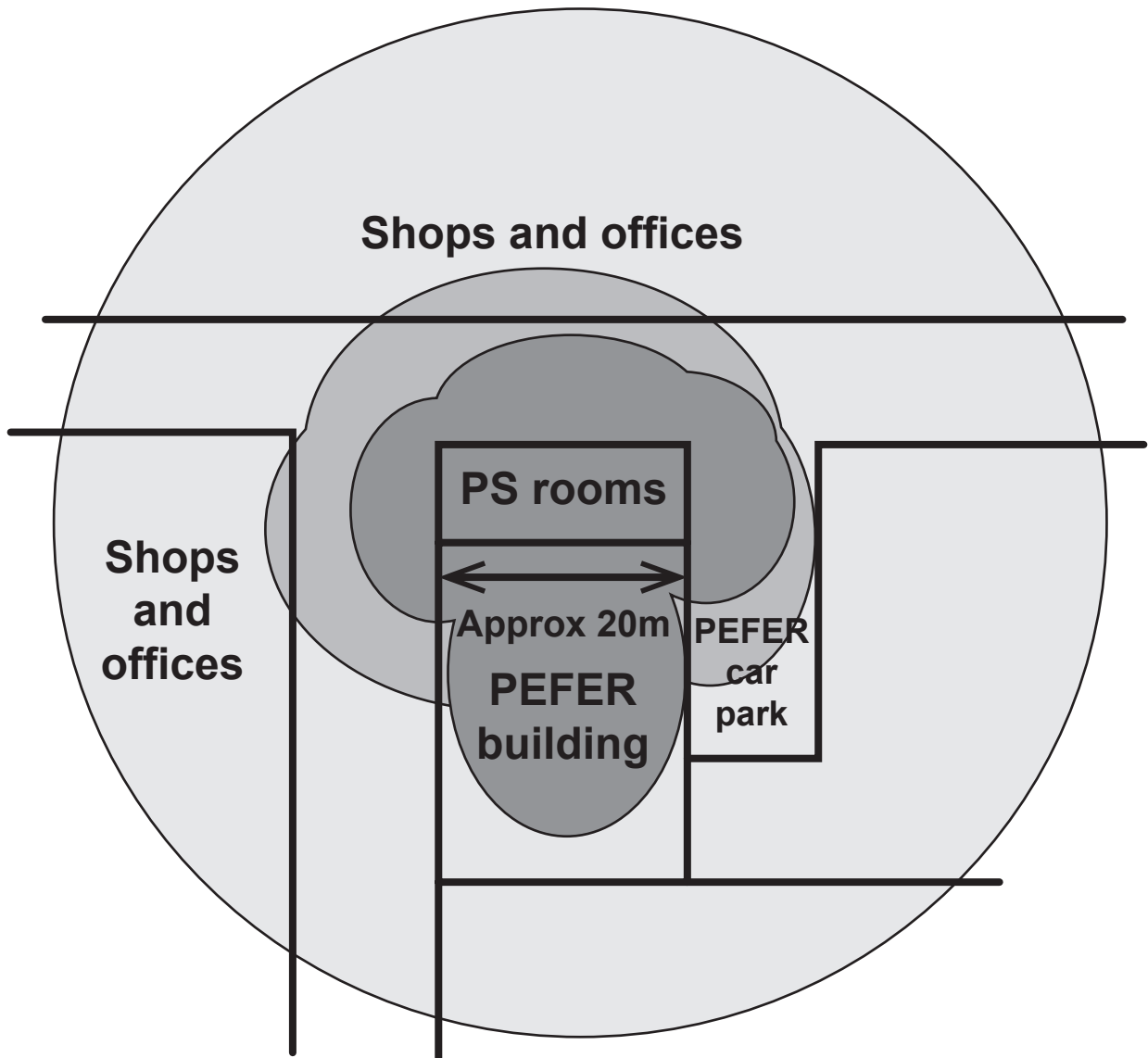
The 29 address means it's a class A network that belongs to the Defense Information Systems Agency.

The router firmware is the latest available version and the router has been out of support since 2015, so I don't think there is much to be done except perhaps change the router.

---

continued on the next page . . .

#### 4 WIFI MAP AND NOTES



Expected range (unobstructed)

Detectable signal, no login possible

Detectable signal, login possible

Turn over

**Notes:**

- i. Coverage lobes estimated from Mlle Maubour's measurements. There could be up to a 5m error in coverage shown**
  - ii. CCTV covers the three sides of the building but only for 5m from the wall. The car park has complete CCTV coverage.**
- 

**continued on the next page . . .**

## **5 CYBER SECURITY DOCUMENTATION – INCIDENT MANAGEMENT POLICY**

### **INCIDENT MANAGEMENT POLICY**

#### **INCIDENT MANAGEMENT TEAM**

**Computer Security Incident Response Team (CSIRT)  
will be:**

**Professor F Gorse and/or Professeur A Lefebvre  
Older member, available from the PEFER IT team  
One or more members of the Projet Serendipity  
board**

#### **EVENT REPORTS**

**Some employee who thinks that an IT security  
incident has occurred should report it as soon as  
possible to the head of the CSIRT (Computer Security  
Incident Response Team).**

**Initially, it can be reported orally, but it must be followed  
by an email.**

**The CSIRT is responsible for keeping detailed  
documentation of the incident from the first report to the  
final solution.**

**Turn over**

**Security incidents can include:**

**Theft of PS equipment**

**Theft of PS data**

**Unauthorised access to the PS's computer systems**

**Infecting the PEFER's computer systems with malware.**

## **INCIDENT RESPONSE PROCEDURE**

### **a) Theft of computer equipment**

**Theft of computer equipment is a very serious problem. All thefts must be reported to the CSIRT official immediately. As a first step, an oral report must be prepared, followed by an email with as much information as possible (location and type of equipment, date of last visit, etc.).**

**The CSIRT team leader needs to check if the item was actually stolen (or just missing).**

**If the theft is confirmed, CSIRT's team leader must inform the police and contact the finance department to inform the insurers.**

**The CSIRT must provide the directors with a report of the theft and, where appropriate, justify the finances required to replace the stolen item.**

**Turn over**

**b) Theft of PS data**

The theft or loss of PEFER's data equipment can be done in several ways. Any loss of PS data must be reported immediately to the head of the CSIRT team, as a first step, and must be followed by an oral report by email.

The CSIRT must investigate the loss and pinpoint what data was lost or stolen, and when the incident took place.

After identifying what has been lost or stolen and when, the CSIRT needs to restore the backups and recover the data as soon as possible.

The CSIRT should review the incident and implement procedures to prevent future losses.

**c) Unauthorised access to PS systems**

Employees suspecting unauthorised access to a computer system must immediately report this to the CSIRT team leader, specifying as much detail as possible (which system has been accessed). First, an oral report must be prepared, followed by an email.

continued on the next page . . .

**Turn over**

**The CSIRT will conduct a thorough investigation of the incident and determine how unauthorised access has occurred.**

**The CSIRT will take all necessary measures to prevent future events (e.g. change passwords).**

- d) Infection of PS computer systems with malware**  
**Employees who suspect that a computer system has been infected with malware must immediately report to the CSIRT Team Leader. As a first step, an oral report must be sent by email.**

**The infected system should be shut down as soon as possible.**

**The CSIRT will examine the infection and take appropriate action to correct the infection and restore the system.**

---